BY ORDER OF THE COMMANDER
AIR RESERVE PERSONNEL CENTER

AIR RESERVE PERSONNEL CENTER
INSTRUCTION 33-2110

15 DECEMBER 2005

Communications and Information

COMMUNICATION SECURITY (COMSEC) USER REQUIREMENTS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: HQ ARPC/SCON (Ms Susan Smith)

Certified by: HQ ARPC/SC
(Mr Stephen J. Hannan)

Supersedes ARPCI33-2110, 20 October 2004

Pages: 14
Distribution: F

This instruction implements Air Force Instruction (AFI) 33-201, Volume 2, *Communications Security (COMSEC) User Requirements*, and Air Force Space Command (AFSPC) Supplement 1 to AFI 33-211, *Communications Security (COMSEC) User Requirements* and 460th Communications Squadron (CS) COMSEC account requirement letters to ensure the proper security of COMSEC material and prescribes procedures for the handling and protection for cryptographic material for Headquarters Air Reserve Personnel Center (HQ ARPC)/Network Operations (SCON). It outlines responsibilities of the unit commander, COMSEC Manager/Alternate and the COMSEC Responsible Officer (CRO) to ensure accomplishment of actions contained herein. It applies to all HQ ARPC personnel. The COMSEC Manager must periodically review this instruction at least every 3 years. All personnel with access to COMSEC material must be familiar and comply with the procedures listed here and in applicable COMSEC publications. A bar (|) indicates revision from the previous edition.

SUMMARY OF REVISIONS

This revision removes numerous AFI references that have been incorporated in existing AFIs. A procedural change instructing specific pick up days for COMSEC materials has been deleted. Equipment identification references have been changed from KY-57 to KIV-7 in paragraph **12.1.** The approved shredder location is changed in paragraph **14.10.** The 460th office symbol in paragraph **18.1.** has been updated. Secret Internet Protocol Router Network (SIPRNET) and Tactical Fastlane (TACLANE) problem phone number is changed; the KG-175 equipment identified is deleted in paragraph **18.2.**

1. References.

1.1. AFI 31-401, *Information Security Program Management.*

1.2. AFI 33-201, Volume 9*, Operational Instructions for Secure Voice Devices*.

1.3. AFI 33-201, Volume 4, *Cryptographic Access Progra.*

1.4. AFI 33-201, Volume 2, AFI 33-211/AFSPC Supplement 1.

1.5. AFI 33-201, Volume 3, *Reporting COMSEC Deviations*.

1.6. AFI 33-215, *Controlling Authorities for COMSEC Keying Material (KEYMAT)*.

1.7. AFKAG-1*, Air Force Communications Security (COMSEC) Operations*.

1.8. AFKAG-2, *Air Force COMSEC Accounting Manual*.

1.9. *Air Force Systems Security Instruction 3021*.

1.10. *Operational Security Instruction for the AN/CZY-10/10A Data Transfer Device (DTD.*

1.11. AFI 33-201, *Communications Security (COMSEC.*

1.12. AFI 33-201, Volume 5, *Controlled Cryptographic Item (CCI)*.

2. Responsibilities. The CRO is responsible for maintaining this instruction with its emergency actions and various attachments. The 460 CS provides all COMSEC materials required by HQ ARPC/SCON.

3. Training.

3.1. The CRO is required to maintain an AF IMT 4168, **COMSEC Responsible Officer and User Training Checklist** (LRA), on each individual granted user access to COMSEC materials. The CRO and users must be aware of this plan and be familiar with the various applicable duties. Familiarization will be accomplished through semiannual reading. The review is documented on AF IMT 4168, and will be retained on file for 2 years, or from one Command Functional Review to the next.

3.2. The Primary and Alternate CROs will be trained by COMSEC account personnel.

3.3. The CRO will train all personnel listed on their COMSEC access letter.

3.4. The CRO will establish a comprehensive, recurring semiannual training program.

3.5. Training will include:

3.5.1. Semiannual review of AFI 33-201, Volume 2.

3.5.2. Semiannual review of COMSEC Operating Instructions.

3.5.3. Semiannual review of COMSEC Emergency Action Plans.

3.5.4. Semiannual review of the COMSEC User Guide.

3.5.5. Semiannual review of the COMSEC equipment security doctrine and operating instructions.

3.6. The training will be documented on a single AF IMT 4168. Additional training may be included:

3.6.1. Conduct and document semiannual COMSEC Emergency Action Plan dry-run exercises.

3.6.2. Refreshers will be given prior to issue and deployment.

4. Receipt Procedures.

4.1. Only the CRO or Alternate CRO are authorized to pick-up COMSEC from COMSEC Account 623003, according to the COMSEC Authorization Appointment Letter.

4.2. The CRO will coordinate with COMSEC Manager to pickup COMSEC material.

4.3. Take a briefcase to courier the COMSEC material, CRO appointment letter, and ID.

4.4. Ensure the short title, edition, quantity, and register number(s) of the material match each entry on the SF 153, **COMSEC Material Report**. If the material is incorrectly listed, bring it to the attention of the COMSEC account personnel.

4.5. When page checking, verify the presence of each page as listed on the list of effective pages and annotate the completion in the record of page checks table or on the front cover.

4.6. Verify the presence of segment 1 in the window of a keytape canister. If there is no canister, account for each segment.

4.7. Sign the hand receipt in the appropriate block once you have accounted for all the material listed.

4.8. Return immediately to your work place (Buckley Annex) with the COMSEC aids, making only emergency stops. Keep the material under your personal control until properly relieved of it, or until such time it can be stored in a security container.

4.9. Upon return to your work center, immediately place all material on your AFCOMSEC Form 16, **COMSEC Account Daily/Shift Inventory**, show visible addition with a **GREEN** ink pen, inventory the material, and secure it in your designated security container SC-8 at post 2-F-21.

4.10. Maintain all hand receipts until all materials have been destroyed or returned to the main account. Line through items that have been destroyed or returned. Indicate in the remarks column: "*destroyed*" or "*returned*", date, and your initials. When all items listed on a hand receipt have been destroyed or returned, remove it from the accounting folder.

5. COMSEC Material Accountability.

5.1. All COMSEC materials and equipment brought into or taken out of the HQ ARPC/SCON account will be controlled/signed for on SF 153. The SF 153 will be used anytime materials are transferred or issued.

5.2. All COMSEC material will be physically inventoried when the safe is closed at the end of the duty day using AFCOMSEC Form 16.

5.3. All COMSEC material will be listed on AFCOMSEC Form 16 for inventory and accounting purposes.

5.4. A new form will be prepared the first duty day of each month.

5.5. Record the short title, edition, quantity, and register number of each Accounting Legend Code (ALC) 1 COMSEC item.

5.6. ALC 4 material will be recorded in the same manner as ALC 1.

5.7. Account for each COMSEC item by comparing the short title, edition, quantity, and register number with the entry on the inventory. Place a mark in the appropriate block for each item and your initials under the corresponding day/shift that the safe was opened.

NOTE: When inventorying keying material, check the segment number in the window and account for all previous segments on the Disposition Record Card.

5.8. Inventories will be performed on the days that the safe is opened, just before you lock the container for the final time that day.

5.9. Do not use whiteout, correction tape, or erasures to correct errors. Neatly line through, initial, date errors. Record explanatory remarks on the back of the form and certify it with your initials.

5.10. Use only blue or black ink (no pencil).

5.11. The CRO must review inventories monthly to make sure they are properly documented, before they are filed. Document the reviews (e.g., reviewed by date and initials) on the back of the AFCOMSEC Form 16. Maintain the current inventory plus the previous 6 months.

6. COMSEC Access Controls and Procedures.

6.1. CROs may grant access to individuals who possess the appropriate security clearance and need-to-know.

6.2. The CRO will use the Automated Security Clearance Approval System (ASCAS) roster or Sentinel Key print out to verify security clearances. The CROs must review the COMSEC access list monthly to ensure its accuracy and then mark the review date and their initials on the list. Access will be denied to anyone losing his or her clearance.

6.3. The CRO will limit unlimited access to COMSEC material in a user facility to persons named on the official access list.

6.4. Only those visitors with a valid need may gain access to the COMSEC safe (COMSEC Account personnel and Major Command inspectors). These visitors must sign the AF IMT 1109, **Visitor Register Log**, and must be escorted at all times.

6.5. Two-Person Integrity (TPI). Two individuals authorized COMSEC access must be present at all times while a TPI key tape is issued (i.e., removed from its canister). Two authorized personnel must initial for issue and destruction. The National Security Agency (NSA) canister counts as a second person until the key segment is issued, at which time it becomes TPI and must have two cleared individuals with it at all times. Once it is destroyed and annotated on the proper form, place the canister back in the safe.

6.6. When TPI is received for HQ ARPC/SCON, another appropriately cleared person must inspect the packaging to determine if it has been tampered with and document the inspection on the user's copy of the SF 153.

6.7. All COMSEC material used at HQ ARPC/SCON will be picked up from the 460 CS COMSEC Account. Arrangements for picking up COMSEC material are made with the 460 CS COMSEC office. The individual who picks up the COMSEC material will ensure all of it is logged on the AFCOMSEC Form 16. Two appropriately cleared individuals will destroy this material at the time of supersession, or the first duty day after supersession occurs. The SF 153 will be delivered or faxed to the COMSEC Account no later than 1 duty day after destruction.

7. Transfer of Accountability. These procedures ensure the transfer of accountability of COMSEC material from the present CRO to the successor.

7.1. Purpose: To ensure prior to permanent departure from the work center (e.g., Permanent Change of Station (PCS) Permanent Change of Assignment (PCA), etc.). These instructions are applicable to all personnel with an active hand receipt for COMSEC material.

7.2. Procedures. An updated "COMSEC Authorization Appointment Letter" will be accomplished and forwarded to the COMSEC account a minimum of 30 days prior to CRO changeover. This letter must be on file prior to allowing a person to sign for COMSEC material.

7.3. The CRO or alternate will contact the COMSEC account during duty hours to advise them a new hand receipt will be required. The rank and name of the individuals signing for the material will be provided.

7.4. At the designated time, the individual assuming CRO duties will report to the COMSEC account for an initial briefing and training. The newly prepared hand receipts will be provided at that time. A thorough physical inventory will be accomplished, by the new and old CRO, on the user account using the new hand receipts. Page checks of all paper material must be performed and documented. The original copies of the new hand receipts will be hand carried back to the COMSEC account for records clearance. Discrepancies will be brought to the attention of the current CRO and/or the COMSEC account, as appropriate. Errors corrected on hand receipts require two authorized individuals' initials.

7.5. It is recommended that a self-inspection of the entire sub-account be accomplished using AF IMT 4160, **Information Assurance Assessment and Assistance Program (IAAP) Criteria**. This will provide the new CRO a detailed view of the status of the account.

8. Physical Security.

8.1. Maximum security must be maintained at all times. COMSEC material must, unless personnel safety is jeopardized, be secured or kept under guard, regardless of the type of emergency.

8.2. COMSEC material must be stored in an approved General Services Administration (GSA) safe with only those personnel on the COMSEC Access List having access to the safe. Upon opening any safe, the initials of the person opening the safe, date, and time the safe was opened must be annotated on the SF 702, **Security Container Check Sheet**. The same is true each time the safe is closed. When the safe is closed, a second person must check and annotate the safe has been closed on the SF 702. If a second person is not available, the same person will ensure the safe is locked and secure, and annotate the appropriate block on the SF 702. For 24-hour work centers, before the beginning of each shift, an inventory of all COMSEC material must be accomplished. For non 24-hour work centers, the inventory must be performed prior to the safe being closed for the day, (final time of day).

8.3. Combinations to all safes and doors must be changed when someone with knowledge of the combination(s) departs, there is a possible compromise, or at least annually. Safe combination changes need to be annotated on a SF 700, **Security Container Information**, located on the inside of the locking drawer. The SF 700 must be "affixed" to locking drawer.

8.4. Entry Control Devices (Cipher Locks) are for convenience only. They offer no protection from forced entry or surreptitious manipulation. Give the combination only to persons with regular duties in the area.

9. Relieve from Accountability.

9.1. Inform the COMSEC Manager at least 30 days prior to impending change of CRO. This will allow time to train a new CRO.

9.2. The new CRO will sign an account prepared hand receipt to assume responsibility of on-hand COMSEC aids.

9.3. Prior to assuming responsibility, the new CRO **must** complete a functional review with the departing CRO.

9.4. Contact the COMSEC manager if problems are encountered.

9.5. File the report for review by COMSEC Account personnel.

9.6. The COMSEC Manager's clearance will be obtained before the CRO may depart.

10. Security Container Operations.

10.1. Preventive maintenance must be accomplished on the safe every 5 years.

10.2. The CRO is responsible for ensuring that personnel working on the safe do not have access to the safe's contents.

10.3. Safe custodians must conduct a visual inspection of the safe at least annually and every time the combinations are changed. Document on the AFTO Form 36, **Maintenance Record for Security Type Equipment**.

10.4. Change the combinations when someone who had the combinations departs or loses a clearance, but at least annually.

10.5. An AFTO Form 36 and SF 700 must be kept inside of the locking drawer of the safe.

10.6. The SF 700 will be used to record the date of the combination changes and who to contact if the safe drawer is found opened and unattended.

10.7. The SF 702, located on the outside of the safe, will be used to show date, time, and who has opened and closed that drawer.

11. STU-III Operations.

11.1. The STU-III/Secure Telephone Equipment (STE) combines clear and secure voice/data communication functions into one telephone. The Cryptographic Ignition Key (CIK) is a primary feature of the STU-III and the KOV-14 is the primary of the STE. They unlock the terminal allowing a secure communications link to be established. Once the CIK/KOV-14 is inserted into the STU-III/STE, the system becomes classified up to the highest classification the key is cleared for. The STU-III/STE message display window will show the highest classification that may be communicated while in the secure mode. Do not leave the STU-III/STE unattended. HQ ARPC STU-IIIs/STEs are cleared up to SECRET.

11.2. The STU-III is a Controlled Cryptographic Item (CCI) and national COMSEC policy requires it be protected in accordance with AFI 33-201, Volume 5 and AFI 33-201, Volume 9. The STE is not a CCI item when not keyed.

11.3. In the secure mode, the identification (ID) of the terminal contacted will be shown in the STU-III/STE message display window. Always use the ID shown in the window to authenticate the contacted terminal. The security clearance must be validated for any visitor that requests to use a

STU-III/STE. Validate the security clearance by using the ASCAS roster or the Joint Personnel Adjudication System (JPAS) provided by the Unit Security Manager or 460th Security Forces Squadron, and ID card. The visitor must have a clearance equal to or higher than the classification of the STU-III/STE key to make a call. If the visitor does not have a clearance equal to or higher than the STU-III/STE key, an authorized person must make the call, advise the called party of the visitor's clearance, and remain with the visitor throughout the entire call.

11.4. In facsimile (FAX) mode, all procedures in paragraph 7.3. apply. The STU-III/STE must be in secure data mode to receive or transmit classified information. The identification process is the same for FAX as secure voice. The validation process is the same for visitors receiving or transmitting a secure FAX. Security clearances must be validated before any received classified FAX can be released.

11.5. If HQ ARPC/SCON has to be evacuated for any reason, ensure the CIK/KOV-14 is stored in an appropriately cleared storage container, HQ ARPC/SCON Safe # SC-8.

12. Cryptographic Operations.

12.1. The KIV 7 is on-line cryptographic equipment used for encryption/decryption of digital data and teletype traffic in point-to-point, netted, and/or broadcast operations. The KIV 7 is a CCI and national COMSEC policy requires it be protected. If HQ ARPC/SCON must be evacuated for any reason, the KIV 7 must be zeroized. This can be done by switching the ENABLE/ZEROIZE switch to the zeroize position. The key tape used to fill the KIV 7 will be destroyed using an authorized shredder in accordance with emergency action flash card directions, when required.

12.2. The KOI-18, General Purpose Tape Reader, is the fill device used by the HQ ARPC/SCON account for the KIV 7.

12.3. **AN/CYZ-10:** The AN/CYZ-10, Data Transfer Device (DTD), is an ALC 1 item and must be stored in a GSA approved container when key material is loaded into it. The DTD holds electronic cryptographic keys. A DTD will only be zeroized by the user to prevent compromise of the material held on the DTD. ***NOTE***: DTDs can be zeroized with the power button on or off. Accidental zeroization of the DTD is not considered possible. Any zeroization of a DTD is considered to be with intent and will constitute a COMSEC incident.

13. Cryptographic Access Program. This work center has **no** personnel with access to Top Secret Cryptographic materials, and whose duties **do not** require the keying of five or more different types of cryptographic equipment, or who perform duties as cryptographic maintenance, engineering, or installation technicians.

13.1. Each individual on the COMSEC access list must be formally briefed into the Cryptographic Access Program (CAP). Prior to having access to COMSEC materials, each individual must be (1) properly trained (documented on the AF IMT 4168), read and agree to the provisions of AFI 33-201Volume 4, Attachment 2, Cryptographic Access Briefing, and sign an AFCOMSEC Form 9, **Cryptographic Access Certificate (PA)**.

13.2. The original AFCOMSEC Form 9, once signed, goes to the main account and a copy is filed in the COMSEC Binder. Once entered into the CAP, personnel remain so until there are formally removed. Therefore, prior to a PCS/PCA reassignment, separation or retirement, each individual entered into the CAP must report to the program administrator and request that their cryptographic access be administratively withdrawn.

13.3. The CAP administrator signs in Section 3 for administrative withdrawals while the commander signs for suspensions and revocations. The original goes to the main account and a copy is filed in the transitory section of the COMSEC Binder. ***NOTE*****:** The CRO will maintain these forms for 90 days after the date of withdrawal and will then dispose of them by shredding.

14. Destruction Procedures.

14.1. Use only the SF 153 to document destruction of whole editions.

14.2. A witness is required when destroying COMSEC material and aids.

14.3. Destroy used keying material designated Cryptographic as soon as possible, but within 12 hours of supersession. We are authorized to destroy on the first duty day after the weekend or holiday.

14.4. Destroy irregularly superseded maintenance and test keying material when it is no longer serviceable.

14.5. For unclassified ALC 4 material, a witness official is not necessary, but a destruction certificate to maintain accountability is required.

14.6. When destroying superseded keytapes, you must verify the destruction of all previous segments on the disposition record, then destroy the remaining segments, disposition record, and the canister.

14.7. Forward one copy of the destruction certificates for whole editions to the main account. Upon destruction, remove or line off items from hand receipts and indicate their destruction in the remarks column.

14.8. Maintain destruction certificates for current calendar year plus the 2 previous years.

14.9. Show visible removal from the inventory form with a red marker.

14.10. Use the approved shredder in the Personnel Readiness Division, post 2-E-20.

14.11. Smash any canisters.

14.12. Only the COMSEC Responsible Officer or Alternate may destroy COMSEC.

14.13. Only appointed witnesses may witness the destruction.

14.14. Once the Key Tape Canister is ready to be destroyed two witnesses must be present during the entire destruction and sign the SF 153 documenting the destruction.

14.15. When new COMSEC material is issued or becomes effective, the old material is superseded and must be destroyed. Superseded COMSEC material must be destroyed as soon as possible, but not later than 12 hours after being superseded ***(first duty day for non-24 hour offices)***. Destruction of COMSEC material will be accomplished by two authorized personnel; the destruction official and the destruction witness. The destruction must be annotated on a SF 153, signed in the appropriate blocks by the destruction official and witness. COMSEC material destruction will be accomplished using one of the following methods: shredding (in an approved shredder), burning, or pulping. The destroyed material must then be removed from the current AFCOMSEC Form 16.

14.16. TOP SECRET keying material is considered TPI material when it is issued (i.e., removed from its canister). Two personnel will remain with the issued key tape segment and the canister until the segment is destroyed. Two authorized personnel must initial and date the appropriate blocks for issue on the disposition record when a new segment is pulled, and they must remain together with the segment at all times until the segment is destroyed. After the segment has been used, the two individuals will then destroy the segment, and initial and date the appropriate blocks on the destruction record. Place the canister and the disposition record back in the safe after use. Upon completion of the last effective cryptographic period, all remaining key tape segments in the canisters will be issued and destroyed. The destruction must be annotated on a SF 153.

14.17. The TOP SECRET key tapes HQ ARPC/SCON maintains are only TPI when they are issued. In accordance with AFI 33-201, Volume 2, the plastic canister the tapes come in are approved NSA containers and act as the second person until the tape is issued.

14.18. The ALC 1 material is accountable from receipt to destruction or returned to COMSEC account. When ALC 1 material is destroyed, the SF 153 must be filled out in duplicate. The original is sent to the COMSEC account for their records and a copy is maintained at the sub-account. ***The COMSEC account must receive their copy of the SF 153 no later than the first duty day after the destruction***. The requirements for the SF 153 are the same for any destruction.

14.19. ALC 4 material is accountable by quantity. ALC 4 material is destroyed locally and the SF 153 must be filled out in duplicate. The original is sent to the COMSEC account for their records and a copy is maintained at the sub-account. The requirements for the SF 153 are the same for any destruction.

15. Deployment.

15.1. COMSEC may be deployed to support operations.

15.2. Contact the COMSEC Manager to arrange for the additional months of COMSEC.

15.3. Material to be deployed will be recorded on SF 153 and the couriers will sign for the material. The original will be given to the main COMSEC Account, a copy maintained in the CRO file, and a copy included in the COMSEC package.

15.4. Material will be double wrapped and safeguarded until stored in approved containers at storage site.

15.5. Report any problems/compromises to Base COMSEC Account.

15.6. COMSEC will be stored in approved containers and all accounting measures followed.

15.7. Ensure that all personnel issued COMSEC meet requirements and they are trained on proper procedures.

15.8. Destruction procedures must be followed. Once at the deployed site, locate the shredder or set up a burn area. Account for material and perform shift inventories.

15.9. Follow the same procedures for redeployment.

16. Emergency Action Plans.

16.1. Emergency action plans are required for ALC 1 and ALC 2 material.

16.2. Emergency action plans will provide instructions for the protection of COMSEC material during the events of a fire, natural disaster, and bomb threat.

16.3. An Overseas Continental United States Emergency Action Plan will be applicable to deployable work center in support of specific mission or Unit Training Code (UTC) designator mobility package, which requires COMSEC material. Presently HQ ARPC does not have a deployable work center or UTC designator.

16.4. Tasks cards will be developed to make implementation easier.

16.5. These plans will be coordinated with the COMSEC manager every 3 years, or when changes require re-coordination.

16.6. Reviews and training exercises will be conducted every 6 months and will be documented.

17. Reporting COMSEC Incidents.

17.1. Reference AFI 33-201V3. To ensure all personnel are aware of the reporting procedures and terminology for COMSEC incidents or violations.

17.2. The importance of immediately reporting all known or suspected COMSEC incidents cannot be overemphasized. Any instance of known, suspected, or possible compromise, loss, theft, or loss of accountability of COMSEC material must be immediately reported to the CRO. The CRO must **immediately** report any incident that potentially jeopardizes the security of COMSEC material, or the electrical transmission of national security information, to the COMSEC Manager. ***DO NOT DISCUSS A COMSEC INCIDENT OVER AN UNSECURE PHONE. SIMPLY STATE THAT YOU NEED TO SEE THE COMSEC MANAGER FOR OFFICIAL BUSINESS.*** HQ ARPC/SCON personnel must be thoroughly familiar with, and be able to recognize, any COMSEC incident and report it to the CRO.

17.3. Physical Incident. Any loss of control (material out of COMSEC channels but later restored), theft, loss, capture, recovery by salvage, tampering, unauthorized viewing and access, photographing or copying that can potentially jeopardize COMSEC material is regarded as a physical incident.

17.4. Cryptographic Incident. Include equipment malfunction or operator error that adversely affects the cryptographic-security of a machine, auto-manual or manual cryptographic systems. Using a COMSEC key that is compromised, superseded, defective, previously used, or incorrect application of keying material is one example of a cryptographic incident.

17.5. Personnel Incident. Personnel incidents include capture, attempted recruitment, or control of personnel by a known or suspected foreign intelligence entity, or the unauthorized absence or defection of personnel having knowledge of or access to COMSEC information or material. Also included is loss of security clearance and removal from access to COMSEC material for any reason.

17.6. If an incident occurs, the HQ ARPC/SCON unit commander will appoint an inquiry officer to investigate the underlying causes of the incident and to take positive actions to prevent recurrence.

17.7. The COMSEC Manager will advise the commander of the unit committing the violation, in writing, of the requirement to appoint an investigating officer. The COMSEC Manager will then provide the investigating officer with as much assistance as requested.

17.8. HQ ARPC/SCON personnel must be aware of possible COMSEC violations when discussing the following:

17.8.1. Information concerning access control techniques (i.e., passwords, authentication systems, etc.).

17.8.2. Information concerning detailed concepts/procedures for key updating, key generation, and techniques for remote keying of cryptographic equipment.

17.8.3. The effective or supersession dates of COMSEC keying material.

17.8.4. Filled-in operational AFCOMSEC Forms 22 or Destruction Records Certificate and classified keying material.

17.8.5. Identification of COMSEC material suspected of being compromised.

17.9. Immediately report any incident: personnel incidents, or cryptographic incidents. An incident must be reported to the CRO, the commander, and the Base COMSEC manager.

17.10. Do not talk about the incident over the telephone because the incident could be classified. The COMSEC manager will initiate the investigation. Results of the investigation will be given to respective commanders.

18. Maintenance Support. The purpose of this section is to provide procedures for obtaining maintenance support in the event of cryptographic equipment or circuit malfunction. These instructions apply whenever COMSEC equipment malfunctions or requires maintenance support. ***NOTE:*** Under no circumstances, will unqualified personnel attempt to perform maintenance functions on any type of cryptographic equipment.

18.1. Maintenance support for most COMSEC/CCI equipment is provided by the 460 SCS/SCMC, Secure Communications Maintenance workcenter. During duty hours, direct maintenance problems or concerns to the Secure Communications Maintenance workcenter. For after duty hours problems, call the Job Control Center.

18.2. For SIPRNET and TACLANE problems, contact the Schriever NCC at DSN: 560-2212.

18.3. The base COMSEC Account is the primary point of contact for any DTD problems or malfunctions and may be contacted at commercial: 720-847-5712.

18.4. Network Encryption Systems (NES) maintenance may only be performed by the manufacturer's qualified maintenance personnel.

18.4.1. Maintenance personnel are not allowed access to a NES keyed for normal operations. Any NES in need of repair, must be manually zeroized—remove the AC and back-up battery power—prior to shipment back to the manufacturer for maintenance.

18.4.2. If an NES alarm condition cannot be cleared, the NES is considered to be in a failed state and must be afforded protection commensurate with the classification of the FIREFLY keying material it contains. The NES requires protection until the alarm condition has been cleared—as a result of authorized maintenance—and zeroization of the key is assured. Prearrange return of a NES containing classified key for maintenance with the manufacturer and ship according to AFI 33-101, Volume 5.

19. Inspections.

19.1. The Base COMSEC Account (460 CS/SCBI) will conduct inspections of each sub-account semiannually in February and August using AF IMT 4160. Reports will be endorsed by the unit commander and retained until receipt of the subsequent command inspection report.

19.2. Staff Assistance Visits (SAVs). Contact the COMSEC Manager to request a SAV.

19.3. The CRO must properly identify COMSEC functional review personnel and sign them in on the AF IMT 1109 before authorizing their access to COMSEC material.

19.4. A report identifying the user's rating (Satisfactory or Unsatisfactory), findings, and recommended corrective actions will be sent through the CRO's commander to the CRO for a reply back to the COMSEC manager.

19.5. The CRO will document corrective action taken and forwards a written response to the COMSEC manager. Written responses must be coordinated with the CROs commander.

19.6. Functional reports must be endorsed and returned to the COMSEC account within 10 workdays of receipt.

19.7. Conduct self-inspections before each semiannual functional review by the COMSEC Account. The COMSEC manager will not consider findings identified during the self-inspection as long as the CRO can show progress for the past 30 days.

19.8. Keep all COMSEC manager's review reports until the next Command COMSEC Functional Review.

ANN C. SHIPPY, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 31-401, *Information Security Program Management*

AFI 33-201, *Communications Security (COMSEC)*

AFI 33-201, Volume 9*, Operational Instructions for Secure Voice Devices*

AFI 33-201, Volume 4, *Cryptographic Access Program*

AFI 33-201, Volume 2, *Communications Security (COMSEC) User Requirements*

AFI 33-211, AFSC Supplement 1, *Communications Security (COMSEC) User Requirements*

AFI 33-201V3, *Reporting COMSEC Deviations*

AFI 33-215, *Controlling Authorities for COMSEC Keying Material (KEYMAT)*

AFI 33-201, Volume 5, *Controlled Cryptographic Items (CCI)*

AFSSI 3021, *Operational Security Instruction for the AN/CZY-10/10A Data Transfer Device (DTD)* AFKAG-1*, Air Force Communications Security (COMSEC) Operations* AFKAG-2, *Air Force COMSEC Accounting Manual*

Abbreviations and Acronyms

ALC—Accounting Legend Code

AFI—Air Force Instruction

AFSC—Air Force Space Command

ARPC—Air Reserve Personnel Center

ASCAS—Automated Security Clearance Approval System

CAP—Cryptographic Access Program

CCI—Controlled Cryptographic Item

CIK—Cryptographic Ignition Key

COMSEC—Communications Security

CRO—COMSEC Responsible Officer

CS—Communications Squadron

DTD—Data Transfer Device

FAX—facsimile

GSA—General Services Administration

HQ—Headquarters

ID—Identification

IAAP—Information Assurance Assessment and Assistance Program

JPAS—Joint Personnel Adjudication System

NES—Network Encryption Systems

NSA—National Security Agency

PCA—Permanent Change of Assignment

PCS—Permanent Change of Station

SAV—Staff Assistance Visits

SIPRNET—Secret Internet Protocol Router Network

STE—Secure Telephone Equipment

STU—Secure Telephone Unit

TACLANE—Tactical Fastlane

TPI—Two-Person Integrity

UTC—Unit Training Code